銳基電腦顧問有限公司
Anti-Virus, Network Security & Education

Yui Kee Computing Ltd.

Newsletter

June 2007

Contents

F-Secure's consumer products updated to support Windows Vista

F-Secure's flagship consumer product, F-Secure Internet Security 2007 (FSIS2007), as well as the F-Secure Anti-Virus 2007 (FSAV2007) product have been updated to include support for the Windows Vista operating system. The support is now released as a final customer quality release after a thorough process of development and testing, as well as beta-version availability of several months. The solutions can be purchased through web shops during this week and through retailers and resellers during June. For existing FSIS2007 and FSAV2007 customers with valid licenses the updates are downloadable free of charge starting on June 4th from http://www.f-secure.com/vista/consumers/ . The products will also be available as OEM versions at the end of July for PC integrators and resellers looking to add value to their laptop and desktop computer offering.

The updated products include a host of important product fixes and enhancements, but still have the same familiar and simple user experience that F-Secure users all over the world have learned to trust. The meticulous development and testing period has ensured that the products work optimally together with Vista to offer the best possible protection. Beta versions of the product were tested by several thousand beta–testers on their home computers. The new version of the product received excellent feedback on performance, reliability and quality.

With today's invisible, more targeted and profit-motivated threat scenarios there is an even stronger need for intelligent and automatic protection than before. This is why in addition to having one of the best detection rates and most frequent virus signature updates in the industry, F-Secure Internet Security 2007 and F-Secure Anti-Virus 2007 both include F-Secure

DeepGuard, a cutting edge technology for detecting and stopping any potentially harmful activity in your computer.

More information:

Windows Vista Information > Consumers

Technology Crime Discussed in LegCo

Answering a question by Hon. Sin Chung Kai, Legislative Councillor for the IT Functional Constituency, the Hong Kong Government revealed its measures to combat technology crime.

The Secretary for Security, Mr Ambrose S K Lee provided a written answer. Rising technology crime is believed to be directly related to the increasing popularity of internet usage and online games. About half the technology crimes handled by the Police involve inadequate security awareness of online game players.

However, detection rates of technology crimes for the past three years have been low, 20% or less, compared with about 44% overall. The difficulties encountered include the often international nature of technology crimes; and the ease of identity concealment on the internet.

The Police have over 100 officers to investigate technology crime, with 44 officers in the Technology Crime Division of the Commercial Crime Bureau and 12 officers in each of the Technology Crime Units at the five land Regions. The Police have also established the "Technology Crime Initial Response Cadre", which is made up of 120 Cadre Members. Apart from performing their daily duties, these Cadre Members are on stand-by round-the-clock, providing support to frontline investigators as necessary.

The Police have conducted various computer forensics training courses for their own officers, and officers from other law enforcement departments. Since 2005, the Police have conducted a "Computer Forensics Certification Course" twice, and 39 officers passed the course. This year, 22 officers took the new "Application Computer Forensics Course" further enhance their professional capabilities. An introductory computer forensics course has also been started.

The Police have also made efforts to educate the public about computer crime, joining forces with educational institutions, the Education and Manpower Bureau, Office of the Government Chief Information Officer and the Hong Kong Computer Emergency Response Team. Further efforts include highlighting the issues on the "Police Report" television programme and reaching out to the youth by introducing "Junior Police Call Information Technology Security Ambassadors".

Copyright-related cyber crimes are closely monitored by the Customs and Excise Department (C&ED). The CE&D has collaborated with the academic sector in developing monitoring software to further enhance the efficiency of enforcement actions.

Most cases handled by the CE&D involved the selling of copyright-infringing goods on auction sites. No follow-up actions could be taken in most cases because of inaccurate or insufficient details; the items had already been deleted from the internet; or the seized goods were not counterfeits.

The CE&D have fourteen officials trained in cyber crime investigation, divided into two Anti-Internet Piracy Teams (AIPTs).

More information:

LCQ15: Technology crimes

F-Secure Misses First VB100 Award in Four Years

-Secure's Chief Research Officer Mikko Hyppönen has admitted the company made a mistake when submitting its to Virus Bulletin product for testing, "So how come we failed? Because we shipped them a product with an old update file." This is not a problem for ordinary users, as the product will auto-update via the internet when first installed. However, Virus Bulletin tests products on an isolated test system, and the older update missed one sample, resulting in a 99.88% detection rate, enough to deny F-Secure the VB100 award.

John Hawes from Virus Bulletin confirmed the situation, "After retesting with [the latest] updates in place, F-Secure comfortably detected everything on the WildList, and would easily have qualified for the VB100 award had the correct data been supplied. Their customers, with the benefit of automatic updates, would certainly have been protected by this solid and reliable product."

F-Secure has passed the VB100 test sixteen times since 2003, and only failed this latest test.

More information:

Dang

VB100 Test Results Summary

F-Secure Protection Service in Virus Bulletin's June 2007 comparative test

US Spammer Pleads Guilty

Adam Vitale, 26, of Brooklyn, pleaded guilty to spamming 1.2 million AOL users and hiding the true origin of the mail. This violates the USA CAN-SPAM Act and he may be punished by up to eleven years in jail, and a fine of US$250,000. This is less than five minutes jail and 21 cents per recipient inconvenienced.

His accomplice, Todd Moeller, has yet to enter a plea.

More information:

Brooklyn Man Pleads Guilty to Participating in Massive AOL Spam Scheme

Spammer faces 11 years in prison

Kaspersky Lab releases Centrally-Managed Linux Anti-Virus

Kaspersky Lab has announced the release of Kaspersky Anti-Virus 5.7 for Linux Workstation and Kaspersky Anti-Virus 5.7 for Linux File Server. The latest versions of these two applications include support for managing the product's security settings via Kaspersky Administration Kit, a powerful and flexible tool that provides centralised administration of antivirus protection systems on complex networks.

Other features include automatic an update system, flexible configuration and an on-access scanner.

The F-Secure Data Security summary January - June 2007

Security threats cross technology borders towards a new malicious economy; social engineering, bank scams, Cyber War and clever mobile intruders.

The F-Secure Lab saw a steady flow of reports on a vast variety of data security threats during the first half of 2007. The underlying trend to note is the spread of malicious activity across various forms of technology and applications during the 6-month period. It would appear that the parties behind orchestrating security attacks are conquering more and more foothold to build a stronger, sustainable commercial economy based on carefully crafted security attacks targeting consumers, companies and public sector organizations.

Social engineering developed to a new level of sophistication via the Small.DAM Trojan, causing havoc via e-mail in January, 2007. Masking itself under the pretense of shocking headline news, linked to real-life events such as the January storms in Europe, the Storm-Worm spread at an alarming speed across the globe in just one night. The F-Secure tracking System was illuminated across the continents as the Trojan took its course.

The banking industry continued to be a key target for phishing scams. As Trojans become more technically complex, scammers implemented new techniques in their attacks, including content filters that keep closer track of consumers' online banking activity. Such detection methods make it easier and more effective for fraudsters to collect more account details using a variety of methods. However, an industry discussion is gathering pace around a potential solution to banking scams. F-Secure believes that top-level domains inaccessible to scammers, such as .bank, could put a stop to some of the most alarming phishing activity.

The link between cybercrime and real-life political unrest was tightened as a form of "Cyber War" emerged as political rioting caused general unrest in the Estonian capital, Tallinn. Disputes over the re-location of a Russian Red Army monument not only led to arrests over ground, but several governmental and other public sector and media websites were heavily targeted via Distributed Denial of Service (DDoS) attacks by an extremely active network of hackers. Several key sites were rendered unreachable.

Adding to the construction of a stronger malicious economy of sophisticated security breaches, the mobile malware industry became more active during the last 6 months. "Personalised" SMS spam, financial lotteries, and Viver trojans masking themselves as utility programs are some of the examples of the fast-developing mobile scams. New spyware was also reported for some Windows Mobile and Symbian S60 3rd Edition devices.

It is fairly alarming to see increasingly complex mobile trojans and spyware being developed by growing commercial entities, making solid profits to support further development of the malicious economy.

More Information

F-Secure Data Security Wrap-up 2007 January-June

Masters of Their Domain

Stormworm Spread

FBI targets Botherders

The USA Department of Justice and FBI have announced the results of their ongoing "Operation Bot Roast", a cyber crime initiative to disrupt the activities of botherders and dismantle botnets. Investigations have identified over 1 million victim computer IP addresses and are working with industry partners and the CERT Coordination Center to notify the owners of the compromised machines. They hope to uncover additional incidents where the zombies have been used to facilitate other criminal activity.

They caution that the FBI will not contact you online and request your personal information so be wary of fraud schemes that request this type of information, especially via unsolicited emails. Reports of fraudulent activity should be made to the FBI or police, or can be made online at the Internet Crime Complaint Center, http://www.ic3.gov/. It is not made clear whether this URL should only be used for USA crimes.

Three suspects have been charged or arrested as a result of Operation Bot Roast, so far:

- James C. Brewer of Arlington, Texas, is alleged to have operated a botnet that infected Chicago area hospitals. This botnet infected tens of thousands of computers worldwide. (FBI Chicago);
- Jason Michael Downey of Covington, Kentucky, is charged with an Information with using botnets to send a high volume of traffic to intended recipients to cause damage by impairing the availability of such systems. (FBI Detroit);
- Robert Alan Soloway of Seattle, Washington, is alleged to have used a large botnet network and spammed tens of millions of unsolicited email messages to advertise his website from which he offered services and products. (FBI Seattle)

The FBI asserts its continued commitment to aggressive investigation of cyber criminals.

More information:

Over 1 Million Potential Victims of Botnet Cyber Crime

FBI logs its millionth zombie address

Abandonned Websites Host Malicious Code

Brian Krebs of Security Fix found that 33% of websites hosted on nine servers at web-hosting company IPOWER Inc served malware. Most of the sites appeared to belong to individuals and small businesses, and many had not been updated or viewed by their owners for months or years. Extrapolated to all of IPOWER's servers, the company may be hosting nearly a quarter-million malicious Web sites, and the problem is unlikely to be limited to just one hosting provider.

The study followed a report by StopBadware.org, a joint effort by Google, Harvard Law School's Berkman Center for Internet & Society and Oxford University's Internet Institute, which identified more than 90,000 sites that attempt to install malicious software on visitors' computers via Internet browser security holes or programming tricks.

The situation is unlikely to improve until someone is forced to take responsibility. The hosting companies are competing to provide lowest-cost web hosting to small users. The fact that many of their servers are running old versions of server software with unpatched security flaws reflects the strong competition and their tight budgets. The website owners are looking for a cheap, easy way to get onto the web, and probably do not have the technical skills to recognise whether their hosting provider is secure, or if their site has been compromised. Criminals are only too happy to exploit this situation, and host their malware on otherwise innocent sites.

More Information:

Cyber Crooks Hijack Activities of Large Web-Hosting Firm

Introducing Google's online security efforts

Criminals hijack large web hosting firm (Cryptogram)

Teaching Virus Writing is Still a Bad Idea

Four years ago, the University of Calgary announced a course including virus writing, and the anti-virus community, including this newsletter criticised it as a bad idea. Professor George Ledin at Sonoma State Universuty has recently started a similar course.

Our Chief Consultant, Allan Dyer, comments:

It appears that Professor Ledin has thought carefully about this, in a 2005 column in "Inside Risks" he wrote, "Computer science students should learn to recognize, analyze, disable, and remove malware. To do so, they must study currently circulating viruses and worms, and program their own". The only part I disagree with is the, critical, last phrase, "and program their own". Self-replicating code is inherently more dangerous, and instructing students to write it has minor educational value, but very high risks. What should be taught, and what would make graduates highly sought-after by anti-virus companies, is reverse-engineering skills. Any idiot can write self-replicating code (just take a look at the virus writers that have been caught), taking apart a convoluted, obfuscated, badly–written program and correctly determining what it does and whether it is a threat is a much harder skill.

More Information:

Not Teaching Viruses and Worms Is Harmful

University to Teach Virus Writing

Teaching Viruses (Cryptogram)

Innovative Course Leads Students Through Dark World Of Computer Security

Computer viruses invade SSU class -- on purpose

Want to Write a Virus? Take a Class.

Virus catchers

Virus Writing Class?

Computer Viruses Invade SSU Class--on Purpose

Computer viruses invade SSU class -- on purpose

F-Secure shines in both proactive and signature-based protection in independent tests

F-Secure protection technologies have scored high in two recent independent tests. Reliability of protection is the core value that F-Secure solutions provide to their users, and these tests substantiate the ability of F-Secure solutions to live up to this ambition.

One of today's most challenging IT security problems are so called zero-day attacks (new unknown malware for which no signature detection exists).

Recently AV-comparatives tested F-Secure's behavior-based detection technology F-Secure DeepGuard for its ability to stop malware that is not found with traditional signature based virus scanning. F-Secure DeepGuard passed the test winning the "Proactive Protection Award" and was able to block all malware used for the test, proving that DeepGuard is able to do an excellent job of identifying and stopping previously unknown "zero-day" threats. The F-Secure DeepGuard technology is based on pervasive monitoring of program behavior during execution, a method which significantly improves the overall level of protection compared to traditional signature based file analysis. This approach enables the security solution to see beneath the surface of the system to detect and stop threats that were designed to pass all traditional defenses unnoticed.

"Our test consisted of new virus samples for which no signatures yet exist. The fact that F-Secure could stop them all with its DeepGuard technology proves that such a behavior-based analysis of malware during run-time can be quite effective in stopping zero-day threats", says Andreas Clementi, project manager at the AV-Comparatives test laboratory.

Despite the importance of behavior-based protection, a core capability of any antivirus solution is the ability to detect malware that is known and can be identified with traditional signature based virus scanning. A test done by AV-Test.org in May 2007 included over 600.000 malware samples. F-Secure achieved a very high detection rate, and was able to detect 978 samples more than Symantec, 42,226 samples that Trend Micro did not detect, and 64,653 samples more than McAfee. F-Secure also detected 105,391 samples that Microsoft's solution missed.

"F-Secure is a challenger in the global antivirus market, and as such we need to perform better than our big competitors. Our systematic focus on innovative protection technology development and state-of-the-art research coupled with highly automated proprietary analysis systems is producing results that our customers see as a very highly reliable protection of their PC's and smartphones" says Pirkka Palomäki, Senior Vice President of Research and Development at F-Secure.

More Information:

AV-Comparatives

AV-Test.org

Whitelisting and the Decline of Anti-Virus

In an article published in The Register, consultant Robin Bloor argues that the time for anti-virus has passed, and the future is security through whitelisting. He points to the recent acquisition of SecureWave by PatchLink as demonstrating the rise of whitelisting vendors; suggesting that there is no need at all for AV once you have whitelisting and, "we'll never stop the global virus plague until AV becomes defunct".

While the business implications of the acquisition will be interesting to financiers and investors, security experts and IT users should look at the technical and social implications, in particular:

- Control and Flexibility
- Defence in Depth

Whitelisting enforces what software is allowed to run on a machine. The controller of the centralised list would wield enourmous power. Suppose it was controlled by a company, call them "Monopolistic Software", how could competitors and open source developers get a guarantee of fair treatment in the validation process? Anti-virus does not have this problem because preventing a rival's software from running would require a positive act, blacklisting, that can be verified, demonstrated and used as evidence in court. The unfairness of "delays" in validation could be glossed over.

Then there is the problem of what happens when bad software is validated. It will happen, developers will be running unprotected machines, or they wouldn't be able to run the software they are creating, and some devlopers will be malicious. Whitelisting is therefore a fragile "solution", that does not cope well with failure.

In fact, the function of "Perfect Anti-virus software" is exactly the same as "Pefect Whitelisting software", they allow good programs to run, and stop bad programs from running. As we know that it is impossible to create "Perfect Anti-virus software" (Dr. Cohen provided a mathematical proof), we know that "perfect Whitelisting software" cannot exist. We live in the real world. Design your security strategy with defence in depth to cope with the imperfect solutions we have available.

29th June 2007

The comments on The Register article are well worth reading, Vesselin Bontchev points out the flaws in whitelisting and Trusted Ownership. One commentator dramatically demonstrates his ignorance by questioning Dr. Bontchev's expertise, rather like saying Stephen Hawkins doesn't know physics!

More Information:

The decline of antivirus and the rise of whitelisting

Comments on ‘The decline of antivirus and the rise of whitelisting’

Huyi Claims Internet Population Explosion

In their sales brochure, Huyi Global Information Resources (Holding) company claims that the Internet Keywords it sells exclusively in Hong Kong provide access to "303,000,000,000 million Netizens". Therefore, according to Huyi, the population of the internet is over Forty-Million times the population of the World!

Other claims made by Huyi that have yet to be independently corroborated are:

- Huyi has been appointed by China Internet Network Information Center (CNNIC), the state network information center of China, as the exclusive Registrar for .CN, .中国, .公司, and .网络 domains and Chinese Internet Keywords in Hong Kong.
- An unnamed company has applied for the domains 銳記.中国 and 銳記有限公司.中国; and the Internet Keywords 銳記 and 銳記有限公司

As a company with a possible interest in those domain names and keywords, Yui Kee was given five working days to object and make a counter-application. We did not object and, after two weeks, the domain names remain unregistered. Is Huyi creating fictitious applications to scare companies into registering unneeded domain names?

Huyi is being asked to comment on this article, we hope to publish their response in due course.

28th June 2007

Jeffrey Poon of Huyi has responded:

Refer to the article in your company's newsletter, I apology for the unclear explanation for the number of Netizens and the translation mistake in the Leaflet (English Version).

The original intention of the message "HK$ 2.4 per day access to 303,000,000,000 million Netizens through Internet browser and partners search engines.", your website will have the opportunity to reach 303,000,000,000 Netizens per month after the Internet Keyword Service is registered.

Please take a look in the Chinese Leaflet attached, which got a clear explaination. And in the mean time, we are going to revise our English version leaflet to avoid misleading.

Refer to the second question, the aproval procedure is handled by CNNIC, there are unsuccessful applications if applicant doesn't provide adequate information relating to captioned domain name. For example, applicant has to divert the domain name to a website which has the "name" shown on the webpage.

More Information:

CNNIC China Internet Network Information Center (CNNIC)

互易在線 (Huyi)

Kaspersky Lab presents a new analytical article 'The Evolution of Self-Defense Technologies in Malware'

Kaspersky Lab, has released an analytical report: 'The Evolution of Self-Defense Technologies in Malware', by Alisa Shevchenko, a senior malware analyst.

As antivirus protection has developed, virus writers have been forced to find new methods which their creations can use to protect themselves.

Malware self-defense mechanisms can fulfill one or more tasks, including hindering detection of a virus using signature-based methods; hindering analysis of the code by virus analysts; hindering detection of a malicious program in the system; hindering the functionality of security software such as antivirus programs and firewalls.

In her article Alisa Shevchenko tracks the evolution of malware self-defense techniques in the face of increasing pressure from antivirus solutions, and investigates which techniques are likely to develop further.

Until recently, antivirus solutions only analyzed file code, and due to this, the first self-defense technique seen was modification of code in malicious programs. This led to polymorphism and metamorphism, which allow a malicious program to mutate when creating a copy of itself, while retaining full functionality. Naturally, this significantly hinders detection. The article also includes an overview of other self-defense technologies such as code encryption and obfuscation; these technologies are used in order to hinder analysis of malicious code, and when implemented in specific ways can be seen as a type of polymorphism.

Another approach which can be used to hinder detection is the use of packers: dedicated programs which compress and archive files. Packers are commonly used and the variety of packing programs and their level of sophistication continue to grow. Many modern packers, in addition to compressing a source file, also equip it with additional self-defense functions aimed at hindering unpacking and analysis of the file using a debugger.

Malicious programs may also defend themselves against detection by masking their presence in the system. This approach was first used by malicious code for the DOS operating system in 1990, and is now called stealth technology. At the beginning of the new millennium, this approach evolved, resulting in so-called rootkit technologies for the Windows operating system. A large number of rootkits have mechanisms which modify a chain of system calls. Another common type of rootkit technology modifies system data. Modern rootkit technologies aim towards the virtualization and use of system functions – in other words, penetrating even more deeply into the system. Although rootkit technologies do appear to have a future, it's unlikely that they will become highly evolved or widespread in the near future.

Over time, polymorphism and related technologies became less appropriate to the task at hand. The evolution of antivirus technologies has led to signature based detection methods being squeezed out by behavioral detection methods, and as a result, modifying code is less likely to protect malicious programs from being detected. For the vast majority of today's Trojans, which are unable to self-replicate, polymorphism is not an effective means of self-defense. The appearance of behavior analyzers has caused malicious programs to target specific functions in antivirus solutions. "Of course, sometimes self-defense mechanisms are the only solution; otherwise they would not be so common, as they pose too many disadvantages from the viewpoint of maximum, full-scale defense" notes the author.

On the other hand, some techniques designed to hinder code analysis (e.g. obfuscation), continue to be regularly implemented, in contrast to polymorphism. However, the fact that malicious programs are basically powerless in the face of behavioral analysis points to a likely evolutionary path. Alisa Shevchenko believes that virus writers will learn how to make their creations more 'self-aware', enabling them to evade detection by behavior analysis.

The article concludes with a range of forecasts, including a list of which self-defense technologies are likely to evolve more actively than others:

- Rootkits are moving towards exploiting equipment functions and towards virtualization. This method, however, has not yet reached its peak and probably won’t become a major threat in the years to come, nor will it be widely used.
- Technology which blocks files on disk: there are two known proof of concept programs that have demonstrated that we can expect this area to develop in the near future.
- The use of technologies that detect security utilities and interrupt their performance is very common and widely used.

The standoff between cyber criminals and virus writers can be seen as an arms race, in which the achievements of one side will be matched by increasing activity on the other side. In the past few years, there has been an increase in malicious code which is allegedly proof of concept, and which is able to evade security solution. The author believes that such proof of concept code simply adds fuel to the fire: users start to worry about how well their systems are protection, and antivirus developers have to invest more and more resources into combating these supposedly undetectable programs.

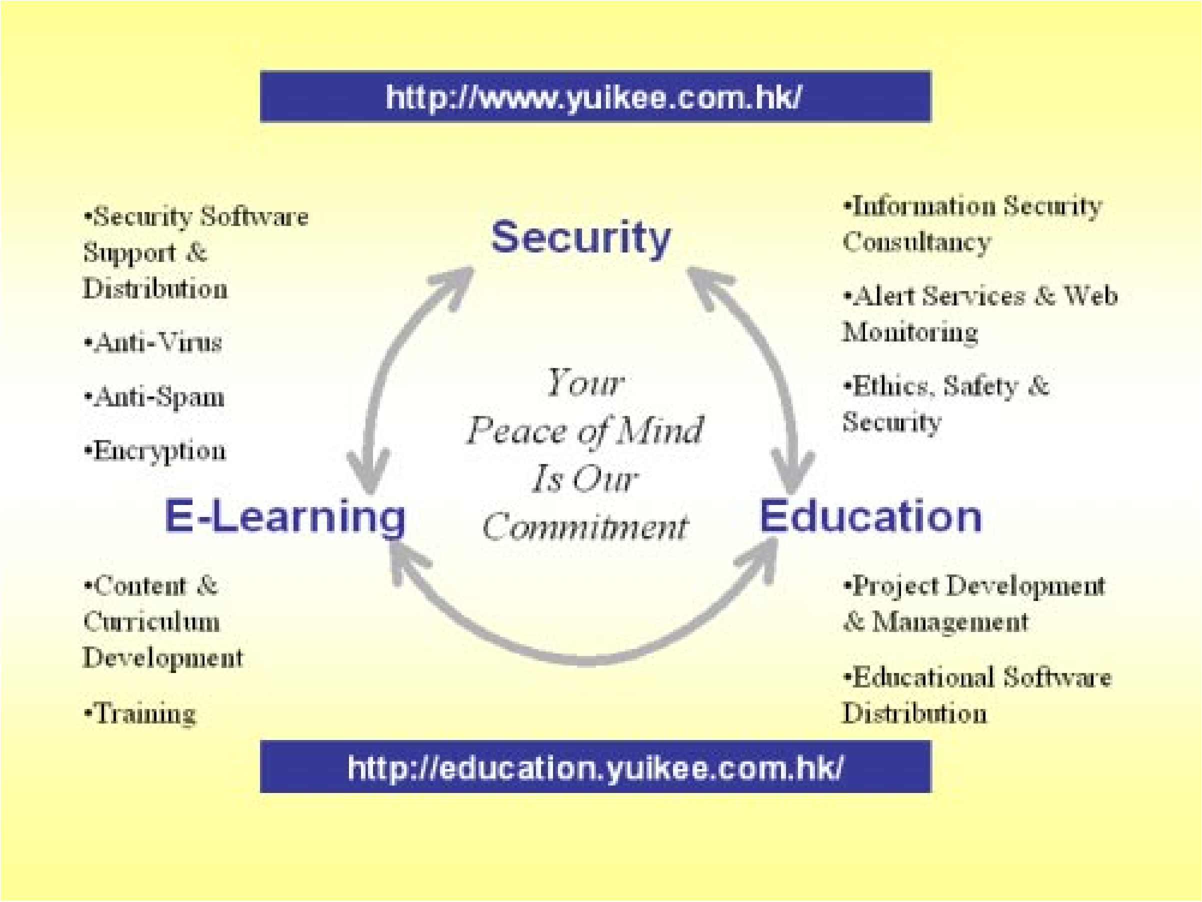
In conclusion, Alisa Shevchenko states that although there is no foreseeable end to the arms race between virus writers and antivirus companies in the near future, if all those involved make an effort, it will be possible to slow the process down.

More Information:

The evolution of self-defense technologies in malware

YUI KEE
銳基電腦顧問有限公司
Anti-Virus, Network Security & Education

Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2870 8550 Fax: 2870 8563
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/



http://www.yuikee.com.hk/

Security

- Security Software Support & Distribution
- Anti-Virus
- Anti-Spam
- Encryption

- Information Security Consultancy
- Alert Services & Web Monitoring
- Ethics, Safety & Security

Your Peace of Mind Is Our Commitment

E-Learning

- Content & Curriculum Development
- Training

Education

- Project Development & Management
- Educational Software Distribution

http://education.yuikee.com.hk/